Understanding Cryptocurrency: A Story of People, Power, Privacy, and Technology

A Research Paper submitted to the Department of Engineering and Society

Presented to The Faculty of the School of Engineering and Applied Science

University of Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science in Systems Engineering

By

Harish Satya Karumuri

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Kent Wayland, Assistant Professor, Department of Engineering and Society

Introduction:

Cryptocurrency started as an underground internet project with hopes of being a means to electronically transfer money without any mediator in pursuit of individual privacy. Over the course of 30 years, this project has become a sector with a market capitalization of nearly 2 trillion dollars. Major organizations are even pivoting into cryptocurrency-related technologies; Vishal Shah, VP at Meta (formerly Facebook) stated that the company's future product is "exploring new types of ownership models and entitlements to ensure people feel confident they actually own something," further citing non-fungible tokens (NFTs) as an example of buying and selling assets (Meta, 2021). Venture capital funding into crypto-related startups is at an all-time high, with over seventeen billion dollars being invested over 2021(Kochkodin, 2021). However, cryptocurrency has gained a bad reputation through pump and dump schemes for unstable coins, hacks into the overall system, ransomware payouts required only through cryptocurrency, and a lack of regulation of digital art and assets – all of this alongside a massive environmental toll. With these prominent negative outcomes, it can be confusing as to why people care about cryptocurrency in the first place, and why people, businesses, and developers see this technology as something exciting. Truth is, technical architecture is based on the ideals of people who built and coded the technology; in this case, it's an ideal of growing distrust of central authority and concern over data privacy. The technology has been further developed by those who have picked up a baton and want to see their vision propagated further through this new paradigm. To this extent, this paper analyzes the motivations and ideas behind cryptocurrency to identify how the technology has changed over the past 30 years in order.

The Initial Start – A Desire for Privacy

With the start of the internet and massive innovations in cryptography and computing, the 1990s saw the initial development of a few electronic currencies, motivated by a concern over the government's growing power. Information transactions, such as credit card transactions, went through central servers, which could easily be used by government bodies to create a picture of any individual they so desired, reducing the privacy that an individual could have. One possible route to protect this privacy was building tools that can scramble the original message but be decoded by only the intended recipients – a process known as encryption. People who were intrigued by this vision came together in the form of an email list, which formed a movement known as the *cypherpunk* movement. The foundational goal: building encryption and cryptographical tools to "create systems which allow anonymous transactions to take place," where anonymous transactions "empower individuals to reveal their identity when desired and only when desired" (Hughes, 1993). Out of these beliefs, projects like B-Money, Bit Gold, and HashCash had potential as they integrated ideas of a decentralized system into an infrastructure that could conduct electronic transactions but ultimately failed due to technical limitations and fraudulent behavior (Reiff, 2021).

This distrust was exemplified when the United States economy plummeted in 2008. Reports of dubious financial practices emerged, with such malpractice being confirmed in the 2011 Financial Inquiry Crisis report. This Crisis Report published, in detail, the "widespread failures in financial regulation and supervision" and "dramatic failures of corporate governance and risk management" (United States Financial Crisis Inquiry Commission, 2011, pp. xv-xxviii). 26 million Americans lost their homes and $11 trillion dollars of household wealth disappeared over the course of the crisis (United States Financial Crisis Inquiry Commission, 2011, pp. xv-xxviii).

The scale of devastation of the financial sector gave groups like the cypherpunks a concrete reason to distrust the Federal Reserve and the capabilities to protect the common person's assets and act as a mediator between banks and customers.

On October 31st, 2008 a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was sent through the cypherpunk email list, penned under the pseudonym Satoshi Nakamoto. Nakamoto's disdain for central authorities is evident in these papers, as he labeled reversible transactions "degrading toward the merchant-customer relationship due to merchants "hassling them [customers] for more information than they would otherwise need," as consumers could exploit disputing a credit card transaction resulting in chargeback fees for the consumer (Nakamoto, 2008). To circumvent this issue, the now-known "Satoshi Papers" builds off the previous groundwork in electronic currency systems and put together a system such that "fraud would be reduced by making it too computationally expensive to reverse any transaction" (Nakamoto, 2008). This general underlying system is known as the blockchain ledger, and Nakamoto dubbed this specific currency network Bitcoin.

Building An Anonymous Information Transfer System

Centralized, Distributed, and Decentralized Systems

Initial computing architectures were centralized, where a large server accepts a user's requests and processes the data accordingly, such as storing information inside a database or transmitting the data to another user. Centralized software architecture requires fewer hardware resources for hosting software products, as all information travels through one server. However, as the technical landscape has grown, users need software products to be much more available on the internet, so distributed computing architectures were developed to divide and spread computing needs among separate machines. Each machine communicates with the others using

network protocols and independently processes whatever tasks are needed. After the processing tasks are completed, the separate outputs must be merged back together to make sure there is consistency in the overall system state; this process is known as consensus. In addition, if one or several computers go down, the overall system should be able to run. It should be noted that implementing a distributed computing architecture adds significant complexity to the overall system, so organizations need to have enough resources to maintain such computing systems or have a robust enough design to handle the added information pathways.

In application, most modern-day systems have some level of a distributed element to them enabled by large advancements in computing infrastructure. This allows for higher availability of software products and services, meaning users can more easily access these services when desired. For example, looking at Google's Gmail system, if User A sends User B an email, the contents and metadata of said email go through Google's servers through the Google Cloud. However, Google has full control over this architecture and therefore visibility into knowing who User A and User B are. For credit cards, if a customer buys groceries using a Visa card, this transaction needs to go through Visa's servers and be approved under the oversight of the organization. In both of these examples, the mediating organizations can see the profile of the users, which removes the anonymity of the user. This is the main privacy concern highlighted inside Hughes' "A Cypherpunk's Manifesto". The manifesto further argues that people "cannot expect governments, corporations, or other large, faceless organizations to grant [people] privacy out of their beneficence" (Hughes, 1993).

This raises the difference between distribution and decentralization. Distribution is the matter of splitting the computing load across many different computers, while decentralization is about who has control over the system. If any entity in a distributed system had a majority of

power, they could control the overall system, making privacy a moot point by Cypherpunk standards. Therefore, to reach the Manifesto's aim of privacy, all actors within the system need to have the same level of power. Such decentralized and distributed systems exist in the form of Peer to Peer (P2P) networks, commonly used to share files between various users without the need for an intermediary.

The Blockchain

Knowing that some kind of P2P system is necessary to avoid a mediator, the last element in this electronic cash system is to transfer cash. However, this is under the consideration that a user must be able to "reveal their identity when desired and only when desired" (Hughes, 1993). The design of the Bitcoin blockchain had one of the first solutions to have some feasibility of achieving this privacy, making the Satoshi papers extremely influential to the development of cryptocurrency. A lot of these concepts were not completely new to the world of computing when the Satoshi Papers were published, but the key skill was piecing the elements of the system together and effectively communicating these ideas.

Anonymously Exchanging Money

Assume that there exists a group of people who have money, and each person within this group keeps track of a receipt. Whenever these people exchange money with each other, everyone keeps a note of the new transaction made. This receipt is more generally known as a ledger or a within the Bitcoin system.

People are considered to have money based on the totality of transactions on a blockchain, with every user's digital signature acting as a personal wallet. For example, If Person A owes Person B $30, and Person B owes Person A $10, we know Person B should have $20 at the end. When the transaction is validated, Person A and Person B's wallets will reflect the

transaction. The interesting aspect of this means that there isn't anything tangible that is exchanged between one user and another. Instead, the money in everyone's wallets is a calculation determined by every transaction made in the entire system.

Lastly, since everyone is keeping track of every transaction to every user, doesn't this reveal everyone's identity? This is where a concept of asymmetric cryptography comes to play – users have their own digital signature such that the user details are encrypted, which hides the personal information of every user but keeps the transactions itself public. The principle here is that person could reveal their wallet ID, and show that a transaction is truly theirs, using this ledger as evidence. However, if a user does not want to reveal their identity, they will, ideally, remain anonymous among the ledger.

Verifying Transactions

Within a centralized system, society trusts central banks to take care of validating transactions and preventing fraud. However, with the aim of building a trustless system, the collective userbase needs to replace a central bank's functions in order to maintain the integrity of the system – especially when the system scales.

Individual transactions can be verified using a unique output known as the unspent transaction output or UTXO. A hash function (another tool in cryptography) is used in order to convert the data within a transaction and generate an associated value. Another user processes this value to verify that this transaction can actually occur. In order to be able to scale this with many more users, multiple transactions are validated together – this collection of transactions is known as a block.

For each block, users will verify each UTXO. Then, they will race with each other to solve what is essentially a cryptographic puzzle. While this sounds strange at first, the premise

here is to require computational power to be used in order to validate transactions – this plays a factor in preventing malicious users from corrupting the system. This results in new blocks being added every 10 minutes to the overall system – this 10-minute marker was proposed in the Satoshi papers (Nakamoto, 2008). The difficulty of the computational puzzle scales to the number of users within the system.

These blocks are then structured together such that if one transaction is changed, the entire system needs to be changed. Malicious users must capture the majority of the computing power within the blockchain system, and then alter the entire blockchain structure. This does create a vulnerability known as a 51% attack – if a majority of the computing power is held by malicious users, they could theoretically rewrite the ledger history and change transactions. However, this is where some game theory comes into play – the cost of gaining 51% of the computing power is extremely expensive, and even if that is obtained, rewriting the entire history destroys the integrity of the entire system, leading to no financial gain.

Why go through all this effort?

Whoever wins the computational race will be awarded some bitcoins, which is established as the first transaction in the next block that's set up. Users who go through this process are referred to as "mining nodes" in the Bitcoin network.

It should be noted that not everyone transferring money through Bitcoin needs to be a mining node. An interesting proposition arises – why should users invest in hardware and an electricity bill that could *potentially* yield an investment into Bitcoin? This all filters down the fundamental belief in the system from the user – does a person believe that the Bitcoin network is a better form of money management than whatever governing body presides over them? Trust in the system affirms the idea computational work should be done to mine the currency. Even if

someone treats owning bitcoin as an investment for the future, there's an implicit recognition, almost like a social contract, that this system can be trusted.

There's much room for discussion on what exactly money is, and whether cryptocurrency qualifies as a form of fiat money, commodity, or something else altogether. At the very least, participating inside of a monetary system requires an acknowledgment that this medium is valid – those who use bitcoin, or any cryptocurrency for that matter, make an implicit agreement that they trust this hardware and software architectural set up to be a means of transacting information. Using the masses as a means of validating transactions is just as reliable, if not, more than any central government.

The Start of Ethereum

In 2010, Blizzard Entertainment (now Activision Blizzard), the game studio behind the massively multiplayer online game World of Warcraft had drastically decreased the strength of the warlock character class, a playable archetype in the game. This also happened to be Vitalik Buterin's main character, the to-be founder of the cryptocurrency network with the second largest market cap. On this day, he "cried [himself] to sleep" as he had "realized what horrors centralized services can bring" as the massive entertainment company had drastically reduced the power of his character (Buterin, 2019). This moment drew him away from *World of Warcraft,* sparking his disbelief in central authority, leading to the eventual creation of Ethereum.

As entertaining as this narrative is, there's more to this story than Buterin's account of this moment, much of this nuance is found in Buterin's upbringing. Buterin was born during the downfall of the Soviet Union before moving to Canada several years later. Vitalik's father, Dmitry Buterin is a deeply curious individual, learning about programming and computers and later having a deep interest in "entrepreneurship, human psychology, and personal development"

(Fenton, 2021a). Dmitry had first-hand seen the Soviet Union's economic system collapsing around him leading to his own beliefs in the trust in governmental authority, or the lack thereof. Dmitry always shared things he found interesting to his son to let the Vitalik tinker with complex ideas – as the father said in an interview, "I've been just trying to feed him a lot of interesting things and see what resonates" (Fenton, 2021b). One of these interesting ideas was the Satoshi Papers themselves.

Buterin had technical skills, and with ample time after quitting *World of Warcraft*, to work on his own decentralized computing system. This led to the release of the Ethereum whitepaper in 2014. Taking this to a cryptocurrency conference, this whitepaper drew the attention of other skilled professionals, leading to a core group of five individuals (including Buterin) who had started the Ethereum project.

One of these recruited founders was Dr. Gavin Wood – a former Microsoft Researcher with a PhD in music visualization. He joined this project with a core belief that this underlying technology could revolutionize how people and software applications could interact with each other. The original whitepaper envisioned a world where the Ethereum Technology could become a computing architecture for new applications. While this could be a new financial system, it could be something even more, like a new system for "online voting and decentralized governance" (Buterin, 2014). Wood "was largely uninterested" in the Bitcoin papers since they were "focusing too much on the currency aspect rather than the technology" (Wood, 2022). However, the paradigm underlying Bitcoin could "invalidate an awful lot of the way that we work, and have worked for the last few hundred years" – this is what got Wood excited about Ethereum. He wanted to use the underlying technology to push forward, in his eyes, how society uses software applications; the blockchain could become a means to "facilitate transactions

between consenting individuals who would otherwise have no means to trust one another" (Wood, 2104). No matter what reasons or circumstances, people would be able to guarantee a transfer of information. To this end, Wood implemented the main standout feature (alongside a good portion of the initial Ethereum code) – smart contracts.

When buying assets or making agreements, people sign contracts that will then be enforced by a governmental system. While this can work in a variety of situations, it involves a third party that does not adhere to cypherpunk privacy standards. However, consider the possibility that one can "embed contracts" into assets and information which is "controlled by digital means (Szabo, 1997). For example, for a relationship between a car and its owner, " if the owner fails to make payments, the smart contract invokes the lien protocol" which could be some digital mechanism that "returns control of the car keys to the bank" (Szabo, 1997). This idea of a digitally enforceable contract is effectively a smart contract. This idea was written by Nick Szabo, who has a background in computer science and law, worked on BitGold (one of the anonymous exchange systems prior to Bitcoin), was on the cypherpunk email chain, and is even considered by some to be the true identity of Satoshi Nakamoto (Popper, 2015). Szabo's *Idea of Smart Contracts* (1997) is directly referenced in the Ethereum whitepaper, thereby linking Ethereum to the foundational principles of cryptocurrency.

Smart Contracts

Ethereum uses many of the same elements as Bitcoin: the same transaction ledger, with a proof-of-work consensus algorithm to ensure that the chain of transactions cannot be tampered with. Instead of the unit of value being Bitcoin, it is an Ether (ETH). It also uses some optimizations so that verifying a block of information goes from 10 minutes to 12 seconds, such that the system is more scalable.

What changes is the verification process; going back to the verification process for Bitcoin, the unique UTXO value was used in order to validate the payments and finalize the payment process. Processing this UTXO value finalizes a payment, and when multiple transactions are connected together more complex transactions can occur through a rudimentary coding language. Buterin observed this and postulated that a robust programming language for enabling more complex transactions could help not just transfer money, but be the basis for a decentralized software application architecture. This language could help enforce complex transactions of information, and become that Szabo's proposed smart contract feature. In short, UTXO would be replaced by a fully-fledged programming language (in computer science terms, a Turing-complete programming language), and those who decide to validate these transactions would effectively process and run the smart contracts. Several languages were developed by the Ethereum team to accomplish this, but the primary one (which was also developed by Wood) was Solidity (Wood, 2022).

Just like Bitcoin, blocks of transactions are validated using mining nodes. However, more complex smart contract will need more computing resources. Having mining nodes receive a same set amount regardless of the work that is incurred will lead to people not wanting to help validate transactions. This is why Ethereum was designed such that when using smart contracts, it's important to consider that "all programmable computation in Ethereum subject to fees" (Wood, 2022). These fees are called *gas fees*. However, the reward for validating a node becomes the associated gas fees, whiles lies as the incentive to participate in the Ethereum Network. Gas fees need to vary based on the complexity of a smart contract, since it utilizes more computational resources (i.e. more electricity). This variation is defined in an auction-like network.

As a mining node validates a transaction or smart contract, the node can quantify how much computation is being done – this quantification is known as *gas*. When a user makes a transaction, they can propose a rate of ETH to gas which is known as the *gas price*, as well as an upper bound on how much gas can be used for the transaction, which is the *gas limit*. Taking these into account, a miner can chose to validate the node (Peaster, 2020), and the miner will receive ETH equivalent to the *gas used times gas prices* which becomes the *gas fee.* If the mining node uses the same amount of gas as the gas limit, the transaction can no longer be validated, but the gas fees will still be given to the mining node. This supply and demand keep the gas price causing higher gas prices when frequent transactions are made (Mougayar, 2015), and adds a tradeoff for anyone wanting to make a transaction: the more complex or quickly the transaction that's needed to be done, the more a user will need to pay.

Another side effect arises – at times where many transactions are being done, all users wanting to make transactions will need to increase their gas prices regardless of what that transaction is. This adds some difficulty in being able to consistently use the Ethereum blockchain for transactions, predicting what the cost of using it becomes very difficult.

The Road Ahead

Gavin Wood published the Ethereum Yellow Paper in 2014. This paper details the specific technical details that make the decentralized system work. He states that a "disinterested algorithmic interpreter" is "incorruptible" of judgment and that this could be verified by humans through a "transaction log" (Wood, 2014). It feeds on the idea that human judgment is imperfect, and that technology is objective and transparent, especially because of the structure of Ethereum. Wood even goes on to call this yellow paper a version of "crypto-law" (Wood, 2014). At a high level, there's an argument to be made that technology can't be judgmental – it's fair to say that

the code will enact the instructions exactly as provided, which is what is referred to as the "disinterested algorithmic interpreter."

However, this code is written and designed by people, whose biases and ideals inform the architectural and design decisions made. The decisions will define the trade-offs users of this technology are expected to make, and participating in this system is an acceptance of that system, even if it's just a superficial acceptance in an attempt to make some money. On top of this consideration, this technology is very new – Ethereum is a very immature technology, as is all cryptocurrency as a whole. Participating in this blockchain system has the risk that an exploit being found that can drastically change or shift the way a system will operate. Are users will into keep trusting a system that is prone to failure? Bitcoin and Ethereum both serve as deep case studies of the mutual shaping between society and people – if people are operating on this system, there will exist ways for the system to be corruptible or lose some legitimacy.

For starters, removing the central authority requires the system to use so much more electricity, which can translate to an increased carbon footprint. Just with Bitcoin, "the record-breaking surge in Bitcoin price at the start of 2021 could result in the network consuming as much energy as all data centers globally, with an associated carbon footprint matching London's footprint size" (de Vries, 2021). One transaction of Ethereum has an "equivalent to the carbon footprint of 316,716 VISA transactions or 23,817 hours of watching Youtube" (Digiconomist, 2021). If people want to use cryptocurrency currently, they need to acknowledge that this environmental cost that occurs.

In regards to human error when coding, the smart contract feature had an exploit with a specific use case when building decentralized autonomous organizations, which led to millions of ether being stolen. The final decision (based on a vote) was to fork the ledger into two

different chains – many users believed letting the ether remain stolen would be of "significant detriment to the development of the Ethereum ecosystem" while others believed "immutability should be a fundamental principle of the Ethereum blockchain without exception" (Antonopoulos and Wood, 2018, p. 325). Having massive changes like this is bound to create disagreement, and reflects poorly on the underlying technology. The disagreement here was large enough to recognize itself as a new cryptocurrency, known as Ethereum Classic, or ETC. The blockchain with the reversed transaction remained as ETH.

This also shows the difficulty in protecting assets on the blockchain. When things go wrong, people want to fall back towards governments or find ways to returns what was stolen from them – which is what many people. However, one of the core beliefs established by Nakamoto is that chargebacks harm the relationship between consumers and suppliers, and isn't integrated into the technology – reversing a transaction to resolve a theft required splitting the blockchain into two different timelines. People who support Ethereum Classic believed that what was stolen should remain stolen because it maintained the trust in the overall chain, or at least, the original blockchain should not have been altered in anyway, regardless of the situation. Instead supports of ETC would rather support security professionals being in place to help hack the hackers back and return the coins to the rightful owners. Within Ethereum Classic, a group known as the Robin Hood Group (RHG) used the same exploit on the original hacker to retrieve 70% of the stolen ETC, a returned it back to the community (Antonopoulos and Wood, 2018, p. 326).

Cryptocurrency also has a use for more under-the-table dealings, one such example being for ransomware payments, which degrade the soft-power and legitimacy of the cryptocurrency systems as a whole. This conundrum (alongside the idea of having a asset protection from cyber

security professionals) is highlighted by the May 2021 Colonial Pipeline ransomware ransom ware attack, which shutdown the pipeline that served 45% of the East Coast. DarkSide, the group responsible for the attack, wanted millions of dollars as a ransom payment. However, DarkSide had made some errors in producing their ransomware, and security professionals could undo the effects of the ransomware (Dudley & Golden, 2021). Additionally, the Department of Justice was able to obtain DarkSide's digital signature, and reverse the transactions made to return the few ransom payments made the Bitcoin back to the Colonial Pipeline (Romo, 2021). With DarkSide being able to remain private on the Bitcoin network, it makes sense that they want to use Bitcoin as their means of obtaining payments. And once again, we see cyber security professionals fighting the hackers on their turf and relying on governmental agencies to recoup assets.

Despite the ethos around cryptocurrency to be based around "trustless," participating in the cryptocurrency network requires some trust in the system. It's inescapable that cryptocurrency is a deeply immature technology that still has flaws and bugs with how it works. The entirety of the world doesn't also exist only within the confines of this technology, people can use other means to get the information they want, The only asset protection that exists is a constant struggle between security defenders and malicious users or a drastic change to the system as a hole. However, new workarounds and developments and being worked on, whether it be to find ways to reduce the energy cost of conducting crypto, finding ways to further decentralize the technology, or new ways to create and protect assets, and new format of making organizations. People will keep passing the baton in the efforts to create new technology that spreads the values, and perhaps leads to another paradigm that more people will resonate with.

Will this be enough to get people to join the excitement of cryptocurrency, or will people

remain against it? Time will only tell, and there's definitely potential to further analyze cryptocurrency from the perspective of the adoption curve. However, what's clear is the mutual shaping between cryptocurrency technology, and the people who use it, the developers who build it, and organizations who need to find out what their relationships will be to these technologies. The values people hold towards these relationships will define the future of this technology, and whatever the potential people see in cryptocurrency will ultimately define whether people can trust the trustless system.

Disclaimers and Disclosure

As of publication, the author does not own any cryptocurrency or cryptocurrency related assets (such as NFTs).

This paper is indented to give a deeper contextual understanding as to why people might care about cryptocurrency and how the goals of the technology have been developed or shifted over time. The final considerations of paper relate to the social legitimacy of cryptocurrency and blockchain, but it is not a declaration that this technology will or will not be successful. In short, this paper is not financial advice, and should not be treated as such.

References

Antonopoulos, A. M., & Wood, G. W. P., PhD. (2018). Ethereum fork history. In *Mastering Ethereum: Building Smart Contracts and DApps.* (pp. 325–329). Van Duuren Media.

Bloomfield, A. (2022, February) *Cryptocurrency – Bitcoin*. [Lecture slides]. https://aaronbloomfield.github.io/ccc/slides/bitcoin.html#/4/6

Buterin, V. (2019). *Vitalik Buterin*. About.Me. https://about.me/vitalik_buterin

Buterin, V. (2014). *Ethereum Whitepaper*. Ethereum.Org. https://ethereum.org/en/whitepaper/

de Vries, A. (2021). Bitcoin boom: What rising prices mean for the network's energy consumption. *Joule*, *5*(3), 509–513. https://doi.org/10.1016/j.joule.2021.02.006

Digiconomist. (2021, December 30). *Ethereum Energy Consumption Index*. https://digiconomist.net/ethereum-energy-consumption

Dudley, R., & Golden, D. (2021, May 26). *The Colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms*. MIT Technology Review. https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

Fenton, A. (2021a, November 16). *Meet Dmitry: Co-founder of Ethereum's creator Vitalik Buterin*. Cointelegraph Magazine. https://cointelegraph.com/magazine/2021/11/16/meet-dmitry-co-founder-of-ethereums-creator-vitalik-buterin

Fenton, A. (2021b, December 24). *The Vitalik I know: Dmitry Buterin* –. Cointelegraph Magazine. https://cointelegraph.com/magazine/2021/12/23/the-vitalik-i-know-dmitry-buterin

Hughes, E. (1997). *A Cypherpunk's Manifesto*. In The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (pp. 285–287). John Wiley & Sons, Inc.

Kochkodin, B. (2021, June 18). *Venture Capital Makes a Record $17 Billion Bet on Crypto World*. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-18/venture-capital-makes-a-record-17-billion-bet-on-crypto-world

Meta. (2021, October 28). *The Metaverse and How We'll Build It Together -- Connect 2021* [Video]. YouTube. https://www.youtube.com/watch?t=2361&v=Uvufun6xer8

Mougayar, W. (2015, May 24). *The Business Imperative Behind the Ethereum Vision.* Ethereum Foundation Blog. https://blog.ethereum.org/2015/05/24/the-business-imperative-behind-the-ethereum-vision/

Nakamoto, S. (2008) Bitcoin: *A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf

Peaster, W. M. (2020, September 22). *Ethereum Gas Explained.* Defiprime.Com. https://defiprime.com/gas

Pimentel, B. (2021, September 30). *Ethereum co-founder Gavin Wood fights 'crypto nationalism.'* Protocol. https://www.protocol.com/fintech/polkadot-ethereum-gavin-wood

Ravikant, N. (2022, April 14). *Vitalik: Ethereum, Part 2*. Naval. https://nav.al/vitalik-2

Reiff, N. (2021, August 26). *Were There Cryptocurrencies Before Bitcoin?* Investopedia.

Romo, V. (2021, June 8). *How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back.* NPR. https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac

United States Financial Crisis Inquiry Commission. (2011). *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States* (Internet materials; No. 9781607963523, 1607963523). Financial Crisis Inquiry Commission. http://purl.fdlp.gov/GPO/gpo50165 ;

http://purl.fdlp.gov/GPO/gpo3449

Schaffel, C. (2018, August 28). *Want Free Coffee? Your Personal Data Is The Way To Pay | WBUR News*. WBUR.Org. https://www.wbur.org/news/2018/08/28/shiru-cafe-data-providence

Szabo, N. (1997). *The Idea of Smart Contracts*. Nick Szabo's Papers and Concise Tutorials. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum project yellow paper, 151(2014), 1-32

Wood, G. (2022, January 7). *Gavin Wood*. Gavin Wood. https://gavwood.com